APROB
Rectorul USEFS,
dr. hab., prof. univ.
_______________ V.Manolachi
„15" ianuarie 2015

REGULAMENTUL
PRIVIND PRELUCRAREA INFORMAŢIILOR CE CONŢIN DATE CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENŢĂ RESURSE UMANE A UNIVERSITĂŢII DE STAT DE EDUCAŢIE FIZICĂ ŞI SPORT

I. DISPOZIŢII GENERALE

1.1. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență resurse umane (în continuare Regulament) este elaborat în vederea implementării în cadrul Universităţii de Stat de Educaţie Fizică şi Sport a prevederilor Legii nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal, a Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123 din 14 decembrie 2010, precum şi întru respectarea prevederilor art. 91 - 94 ale Codului muncii al Republicii Moldova.

1.2. Prezentul Regulament reglementează condițiile generale şi cerințele fată de prelucrarea datelor cu caracter personal ale angajaților USEFS în cadrul sistemului de resurse.

II. SCOPUL

2.1. Scopul prelucrării informațiilor ce conțin date cu caracter personal în sistemul de evidență resurse umane constă în asigurarea înregistrării informațiilor din secţia resurse umane referitoare la datele personale ale angajaților, inclusiv a categoriilor de slarizare, stimulărilor, sporurilor, indemnizațiilor, compensațiilor şi altor drepturi şi obligații cu conținut pecuniar, precum şi a prezentării rapoartelor statistice trimestriale şi anuale către instituţiile statului, conform legislației în vigoare.

2.2. În cadrul sistemului de evidență resurse umane sînt prelucrate următoarele categorii de date cu caracter personal:

- numele, prenumele şi patronimicul;
- numărul personal de identificare de stat (IDNP);
- data naşterii şi domiciliul;
- studiile (diplome deținute);
- codul personal de asigurări sociale (CPAS);
- datele privind locul de muncă şi funcția ocupată;
- mărimea salariului brut şi alte premii, sporuri, stimulări, suplimente;
- datele privind situația familială (la cererea solicitantului);
- numele, prenumele (după caz, patronimicul) persoanelor care se află la întreținerea persoanei respective (membrii familiei, alte rude şi persoane, după caz);
- numărul poliţei medicale (CNAM);
- datele din certificatele de concediu medical acordate, necesare pentru calcularea indemnizației corespunzătoare de către contabilitate;
- după caz, alte date necesare îndeplinirii scopului menţionat, conform legislației în vigoare.

1.1. Prelucrarea datelor cu caracter personal menționate va fi efectuată pentru realizarea următoarelor scopuri:

a) Prelucrarea informaţiei privind modificările survenite la prelucrarea datelor cu caracter personal ce vizează angajații și care au impact asupra calculării plăţilor salariale, de exemplu: modificarea gradului de calificare a cadrelor didactice în dependenţă de titlurile didactico-ştiinţifice obţinute, avansarea în treptele de salarizare, evaluarea performanţelor profesionale ale subdiviziunilor cu acordarea sporului pentru performanţă colectivă, vechimea în muncă în domeniul învăţămîntului;

b) Calcularea salariilor lunare, în conformitate cu legislaţia în vigoare a Republicii Moldova (Hotărîrea Guvernului RM nr.195 din 13.03.2013 privind condiţiile de salarizare a personalului din instituţiile de învăţămînt superior de stat cu autonomie financiară, Hotărîrea Guvernului RM nr.381 din 13.04.2006 cu privire la condiţiile de salarizarea personalului din instituţiile bugetare, Legea nr.355-XVI din 23 decembrie 2005 cu privire la sistemul de salarizare din sectorul bugetar);

c) Prelucrarea certificatelor de concedii medicale ale angajaților în vederea stabilirii indemnizațiilor corespunzătoare;

d) Prelucrarea copiilor ordinelor Rectorului referitoare la personal;

e) Întocmirea anchetei persoanei asigurate REV 1 (anchetă) pentru fiecare angajat ce nu dispune de codul persoanei de asigurări sociale (CPAS) pentru înregistrarea acestora la Casa Teritorială de Asigurări Sociale, filiala Rîşcani pe suport de hîrtie;

f) Prezentarea informaţiei ce vizează evidenţă nominala a persoanelor asigurate angajate la Compania Naţională de Asigurări în Medicină;

g) Asistarea procesului (prin furnizarea informaţiei necesare) pentru completarea periodică (lunară, trimestrială , anuală) a raportului şi dării de seamă privind mobilitatea salariaţilor şi locurile de muncă la Biroul Naţional de Statistică al RM;

h) Eliberarea certificatelor cu privire la activitate, funcţia ocupată, salariul mediu lunar şi acordarea concediilor, la cererea angajaților;

i) Completarea și stocarea fișelor personale de evidenţă a angajaţilor (forma nr.T-2)

1.2. Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate de către USEFS astfel încît să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sînt prelucrate, iar la expirarea termenului respectiv, înregistrările se vor distruge/șterge, în funcție de suportul pe care au fost efectuate. În cazul obligațiilor expres prevăzute de lege acestea pot rămîne la păstrare primind statut de document de arhivă.

1.3. Orice utilizare a datelor cu caracter personal, introduse în sistemul de evidență resurse umane în alte scopuri decît cele menționate mai sus este interzisă.

III. LOCAȚIA ȘI DESCRIEREA SISTEMULUI DE EVIDENȚĂ RESURSE UMANE

3.1. Datele cu caracter personal conținute în sistemul de evidență resurse umane în cadrul USEFS se prelucrează/stochează:

1. pe suport de hîrtie;
2. în format electronic (calculator nr.de inventariere 0130027)

3.2. Prelucrarea informaţiilor în sistemul de evidenţă resurse umane pe suport de hîrtie este structurată după criteriul “mape-dosare”, fiind păstrate în dulapuri, care sînt amplasate fizic în biroul Resurse umane (nr.211) din sediul USEFS, str.A.Doga 22.

IV. DURATA DE STOCARE

4.1. Prelucrarea datelor cu caracter personal în sistemul de evidenţă resurse umane se efectuează pe perioada valabilităţii activităţii angajaţilor USEFS (din momentul semnării contractului pînă la încetarea raporturilor de muncă).

4.2. La expirarea termenelor menţionate în punctul 4.1., datele din sistemul de evidenţă resurse umane sînt păstrate în formă arhivată, în Arhiva universităţii (bir.142) pe perioada stabilită conform Nomenclatorului general de păstrare a dosarelor aprobat de Arhiva Naţională a RM.

V. DREPTURILE ANGAJAȚILOR ȘI PERSOANELOR VIZATE

5.1. USEFS, în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecția datelor cu caracter personal ce le revin angajaților, precum și, după caz, altor persoane vizate.

5.2. În conformitate cu principiile de protecție a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenţie, de opoziție asupra datelor cu caracter personal ce-i vizează, precum şi dreptul de a se adresa în justiție.

5.3. Toate persoanele implicate în activitatea de administrare și/sau prelucrare a informaţiilor din sistemul de evidenţă resurse umane vor respecta procedura de acces la datele cu caracter personal.

5.4. Acordarea dreptului de acces a angajaţilor la informaţiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii USEFS. Informaţiile furnizate vor fi acordate astfel, încît să nu prejudicieze drepturile terţilor. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum și perioada concretă pentru care solicită informaţiile.

5.5. Există posibilitatea refuzării dreptului de acces în situaţia în care se aplică excepţiile prevăzute de lege. Necesitatea de a restricţiona accesul se poate impune în cazul în care există obligaţia de a proteja drepturile şi libertăţile unor terţe persoane, de exemplu, dacă în informaţiile solicitate apar şi alte persoane şi nu există posibilitatea de a obţine consimţămîntul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

VI. MĂSURILE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMUL DE EVIDENȚĂ RESURSE UMANE

6.1. Măsurile generale de administrare a securităţii informaţionale

6.1.1. În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hîrtie sau electronic care conţin date preluate din sistemul de evidenţă resurse umane, aceştia se păstrează în safeuri care se încuie.

6.1.2. La terminarea sesiunilor de lucru, computerele şi imprimantele se deconectează de la reţeaua electrică.

6.1.3. Operatorul asigură securitatea punctelor de primire şi expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele de copiere.

6.1.4. Accesul fizic la mijloacele de reprezentare a informaţiei preluate din sistemul de evidenţă resurse este blocat împotriva vizualizării de către persoane neautorizate.

6.1.5. Mijloacele de prelucrare a informaţiilor preluate din sistemul de evidenţă resurse umane sau soft-urile destinate prelucrării acestora sînt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

6.1.6. Scoaterea şi introducerea mijloacelor de prelucrare a informaţiilor din sistemul de evidenţă resurse umane din/în perimetrul de securitate se înregistrează în registru.

6.2. Măsurile de protecţie a datelor cu caracter personal, prelucrate în sistemul de evidenţă resurse umane, se înfăptuiesc ţinînd cont de necesitatea asigurării confidenţialităţii şi integrităţii acestora, prin protecţie în formă manuală, electronică şi externă.

6.3. Cerinţe speciale faţă de marcare:_toate informaţiile ieşite din sistemul de evidenţă resurse umane, care conţin date cu caracter personal, sînt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi răspîndirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

6.4. Accesul în biroul unde este amplasat sistemul de evidenţă resurse este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program. Accesul în birou este posibil doar cu autorizarea de acces şi cheia de la lacătul mecanic.

6.5. Biroul nu este lăsat niciodată fără supraveghere la ieşirea în exterior, uşa biroului se încuie cu lacătul.

6.6. Înainte de acordarea accesului fizic la sistemul de evidenţă resurse umane, se verifică competenţele de acces.

6.7. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acestea se lichidează, iar datele şi documentele ce se conţin în registrul supus lichidării se transmit în arhivă.

6.8. Perimetrul de securitate se consideră perimetrul biroului în care este amplasat sistemul de evidenţă resurse umane, fiind integru din punct de vedere fizic.

6.9. Computerele sînt amplasate în locuri cu acces limitat pentru persoane străine.

6.10. Uşile şi ferestrele sînt încuiate în cazul în care în încăpere lipsesc angajaţii autorizaţi de administrarea sistemului.

6.11. Amplasarea sistemului de evidenţă resurse umane răspunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

6.12. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemului de evidenţă resurse umane, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele de evidenţă resurse umane, inclusiv posibilitatea deconectării oricărui component TI.

6.13. Computerele, unde este amplasat fizic sistemul de evidenţă resurse umane, dispun de UPS-uri, care sînt folosite pentru încheierea corectă a sesiunii de lucru a sistemelor (componentelor) în cazul deconectării de la sursa de alimentare cu energie electrică.

6.14. Securitatea cablurilor de reţea: cablurile de reţea, prin care se efectuează operaţiunile de transmitere a datelor preluate din sistemul de evidenţă resurse umane, sînt protejate contra conectărilor nesancţionate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sînt separate de cele comunicaţionale.

6.15. Securitatea antiincendiară a sistemului de evidenţă resurse umane: biroul unde este amplasat sistemul de evidenţă resurse umane este dotat cu echipament antiincendiar şi corespunde cerinţelor şi normelor antiincendiare în vigoare.

6.16. Controlul instalării şi scoaterii componentelor TI: se efectuează controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemului de evidenţă resurse umane. La expirarea termenului de păstrare, informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug.

VII. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI DE EVIDENŢĂ RESURSE UMANE

7.1. Este efectuată identificarea şi autentificarea utilizatorilor informaţiilor preluate din sistemele de evidenţă resurse umane şi a proceselor executate în numele acestor utilizatori.

7.2. Toţi utilizatorii (inclusiv personalul care asigură mentenanţa tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului.

7.3. Pentru confirmarea ID-ului utilizatorului sînt utilizate parole. Utilizarea parolelor în procesul asigurării securităţii informaţionale: pe lîngă cerinţele de păstrare a confidenţialităţii parolelor, este interzisă înscrierea acestora pe suport de hîrtie, cu excepţia cazului de asigurare a securităţii păstrării acesteia (plasarea înscrisurilor în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.

7.4. Se efectuează modificarea parolelor de fiecare dată cînd sînt depistaţi indicii unei eventuale compromiteri a sistemului sau parolei.

7.5. Întru asigurarea posibilităţii de stabilire a responsabilităţii fiecărui utilizator, sînt folosite identificatori şi parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de evidenţă a introducerilor greşite ale acestora. După trei tentative greşite de autentificare, accesul este blocat, în mod automatizat.

7.6. Se asigură, pentru o perioadă de 1 */un/* an, păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor şi prevenirea folosirii repetate a acestora.

7.7. În cazul în care raporturile de muncă ale utilizatorului au încetat, au fost suspendate sau modificate, şi, ca urmare, noile sarcini nu necesită accesul la datele cu caracter personal, precum şi în cazul de modificare a drepturilor de acces ale utilizatorului, abuz al utilizatorului de autorizaţii de acces primite în scopul comiterii unei fapte prejudiciabile, absenţă a utilizatorului la postul de muncă pe parcursul unei perioade îndelungate (mai mult de 3 luni), codurile de identificare şi autentificare se revocă sau se suspendă.

7.8. Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal în sistemul de evidență resurse umane, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Acţiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal înregistrate în sistemul de evidenţă resurse umane, încetează automat la expirarea perioadei stabilite în timp (pentru fiecare tip de cont de acces în parte). Se dezactivează automat, după o perioadă de maxim 1 */una/* lună, conturile de acces ale utilizatorilor neactivi, care prelucrează informaţiile din sistemul de evidenţă resurse umane. Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

7.9. În scopul depistării şi evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuieşte cu regularitate, maximum la fiecare şase luni şi după oricare schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor la sistemul de evidenţă resurse umane.

7.10. Folosirea tehnologiilor fără fir, echipamentelor portative şi mobile se autorizează de persoanele responsabile.

7.11. Se impun limite în privinţa persoanelor care au dreptul:
a) să vizualizeze informaţiile stocate în sistemul de evidenţă resurse umane;
b) să copieze, să descarce, să şteargă sau să modifice orice informaţie stocată.

7.12. Toţi angajaţii cu drepturi de acces beneficiază de o instruire iniţială în domeniul protecţiei datelor cu caracter personal.

7.13. Orice activitate de dezvăluire a datelor cu caracter personal către terţi este documentată şi supusă unei analize riguroase în prealabil privind scopul şi temeiul legal a intenţiilor de dezvăluire a unui anumit volum de date cu caracter personal.

7.14. Orice încălcare a securităţii în ceea ce priveşte sistemul de evidenţă resurse umane este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cît de urgent posibil.

7.15. Înainte de acordarea accesului în sistem, utilizatorii sînt informaţi despre faptul că folosirea sistemului de evidenţă resurse umane este controlată şi că folosirea neautorizată a acestora este sancţionată în conformitate cu legislaţia civilă, contravenţională şi penală.

VIII. AUDITUL SECURITĂŢII ÎN SISTEMELE DE EVIDENŢĂ RESURSE UMNAE

8.1. Se organizează generarea înregistrărilor de audit a securităţii în sistemul de evidenţă resurse umane pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

8.2. Se efectuează înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem, conform următorilor parametri:
a) data şi timpul tentativei intrării/ieşirii;
b) ID-ul utilizatorului;
c) rezultatul tentativei de intrare/ieşire – pozitivă sau negativă.

8.3. Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării informaţiilor din sistemele de evidenţă resurse umane,

înregistrarea modificărilor drepturilor de acces ale utilizatorilor şi statutul obiectelor de acces conform următorilor parametri:

a) data şi timpul tentativei de pornire;
b) denumirea/identificatorul programului aplicativ sau al procesului;
c) ID-ul utilizatorului;
d) rezultatul tentativei de pornire – pozitivă sau negativă.

8.4. Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării informaţiilor din sistemul de evidenţă resurse umane, conform următorilor parametri:

a) data şi timpul tentativei de obţinere a accesului (executare a operaţiunii);
b) denumirea (identificatorul) aplicaţiei sau a procesului;
c) ID-ul utilizatorului;
d) specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);
e) tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.);
f) rezultatul tentativei de obţinere a accesului (executare a operaţiunii) – pozitivă sau negativă.

8.5. Se efectuează înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces, conform următorilor parametri:

a) data şi timpul modificării competenţelor;
b) ID-ul administratorului care a efectuat modificările;
c) ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

8.6. Se efectuează înregistrarea ieşirii din sistemul de evidenţă resurse umane, înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:

a) data şi timpul eliberării;
b) denumirea informaţiei şi căile de acces la aceasta;
c) specificarea echipamentului (dispozitivului) care a eliberat informaţia (numele logic);
d) ID-ul utilizatorului care a solicitat informaţia;
e) volumul documentului eliberat (numărul paginilor, filelor, copiilor) şi rezultatul eliberării – pozitiv sau negativ.

8.7. Cazurile de deranjament al auditului securităţii în sistemul de evidenţă resurse umane sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sînt aduse la cunoştinţa persoanei responsabile de politica de securitate a datelor cu caracter personal, care întreprinde măsuri în vederea restabilirii capacităţii de lucru a sistemului de audit.

8.8. Rezultatele auditului securităţii în sistemul de evidenţă resurse umane (operaţiunile de prelucrare a informaţiilor şi mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate şi asigurarea confidenţialităţii şi integrităţii acestora.

8.9. Durata minimă a stocării rezultatelor auditului securităţii în sistemul de evidenţă resurse umane constituie 2 */doi/* ani, în scopul asigurării posibilităţii de folosire a acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigaţii sau procese judiciare. În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

IX. ASIGURAREA INTEGRITĂŢII INFORMAŢIILOR DIN SISTEMUL DE EVIDENŢĂ RESURSE UMANE

9.1. Se asigură identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării informaţiilor din sistemul de evidenţă resurse umane, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestora, protecţia contra infiltrării programelor dăunătoare în soft-uri, măsuri care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus.

9.2. Se utilizează tehnologii şi mijloace de constatare a intrărilor ilegale, ce permit monitorizarea evenimentelor şi constatarea atacurilor, inclusiv asigură identificarea tentativelor folosirii neautorizate a informaţiilor din sistemul de evidenţă resurse umane.

9.3. Se asigură testarea funcţionării corecte a componentelor de securitate a sistemului de evidenţă resurse umane (automat – la pornirea sistemului, şi după caz – la solicitarea persoanei responsabile de politica de securitate a prelucrării datelor cu caracter personal).

9.4. Copiile de siguranţă: reieşind din volumul prelucrărilor efectuate, individual, se stabileşte de către operator intervalul de timp în care se execută copiile de siguranţă a informaţiilor din sistemul de evidenţă resurse umane şi soft-urilor folosite pentru prelucrările automatizate a acestora. Copiile de siguranţă se testează în scopul verificării siguranţei purtătorilor de informaţii şi integrităţii informaţiei indicate. Procedurile de restabilire a copiilor de siguranţă se actualizează şi se testează cu regularitate, în scopul asigurării eficacităţii acestora.

X. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENŢĂ RESURSE UMANE

10.1. Persoanele care asigură exploatarea sistemului de evidenţă resurse umane trec, minimum o dată în an, instruirea cu privire la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

10.2. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii. Se monitorizează şi documentează, în mod permanent, incidentele de securitate în sistemul de evidenţă resurse umane.

10.3. Persoanele care se fac vinovate de încălcarea normelor privind obţinerea, păstrarea, prelucrarea şi protecţia informaţiilor din sistemul de evidenţă resurse umane poartă răspundere civilă, contravenţională şi penală.

XI. DISPOZIŢII FINALE

11.1. Prezentul Regulament este revizuit şi ulterior aprobat de către conducerea USEFS, precum şi modificat la necesitate.

11.2. Prezentul Regulament se completează cu prevederile legislaţiei în vigoare.

11.3. Regulamentul este adus la cunoştinţa angajaţilor contra semnăturii.

11.4. Modificarea şi completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.